Europ. J. Combinatorics (2000) **21**, 981–988
Article No. 10.1006/eujc.2000.0416
Available online at http://www.idealibrary.com on IDEAL

A Family of Partial Difference Sets with Denniston Parameters in Nonelementary Abelian 2-Groups

JAMES A. DAVIS AND QING XIANG

We construct a family of partial difference sets with Denniston parameters in the group $\mathbb{Z}_4^t \times \mathbb{Z}_2^t$ by using Galois rings.

1. INTRODUCTION

A k-element subset D of a finite multiplicative group G of order v is called a (v, k, λ, μ)-*partial difference set in* G (PDS) provided that the multiset of 'differences' $\{d_1 d_2^{-1} \mid d_1, d_2 \in D, d_1 \neq d_2\}$ contains each nonidentity element of D exactly λ times and each nonidentity element in $G \backslash D$ exactly μ times. See [11] for background on partial difference sets.

We will limit our attention to abelian groups in this paper. In that context, a character of an abelian group is a homomorphism from the group to the multiplicative group of complex roots of unity. The *principal character* is the character mapping every element of the group to 1. All other characters are called nonprincipal. Starting with the important work of Turyn [16], character sums have been a powerful tool in the study of difference sets of all types. The following lemma states how character sums can be used to verify that a subset of a group is a PDS.

LEMMA 1.1. *Let G be an abelian group of order v and D be a subset of G so that $\{d^{-1} \mid d \in D\} = D$. Suppose k, λ, and μ are positive integers satisfying $k^2 = \mu v + (\lambda - \mu)k + k - \mu$ (when the identity element is not in D). Then D is a (v, k, λ, μ)-PDS in G if and only if, for any character χ of G,*

$$\sum_{d \in D} \chi(d) = \begin{cases} k & \text{if } \chi \text{ is principal on } G. \\ \frac{(\lambda-\mu) \pm \sqrt{(\lambda-\mu)^2 + 4(k-\mu)}}{2} & \text{if } \chi \text{ is nonprincipal on } G. \end{cases}$$

When the group G is an elementary abelian p-group, partial difference sets in G are closely related to two-intersection sets in projective spaces over finite fields. We proceed to explain this connection.

Let $PG(\ell - 1, q)$ denote the desarguesian $(\ell - 1)$-dimensional projective space over the finite field GF(q), where q is a power of prime p. A *projective* (n, ℓ, h_1, h_2) *set* $\mathcal{O}$ is a proper, non-empty set of n points of the projective space $PG(\ell - 1, q)$ with the property that every hyperplane meets $\mathcal{O}$ in h_1 points or h_2 points.

Let $\mathcal{O} = \{\langle y_1 \rangle, \langle y_2 \rangle, \ldots, \langle y_n \rangle\}$ be a set of n points in $PG(\ell - 1, q)$. If we view GF(q^ℓ) as an ℓ-dimensional vector space over GF(q), then we may think of it as the ℓ-dimensional vector space $V_\ell(q)$ associated with $PG(\ell - 1, q)$. Let $\Omega = \{v \in V_\ell(q) \mid \langle v \rangle \in \mathcal{O}\}$ be the set of vectors in $V_\ell(q)$ corresponding to $\mathcal{O}$, i.e., $\Omega = \text{GF}(q)^* \mathcal{O}$.

For $w \in \text{GF}(q^\ell)$, we define a character of the additive group of GF(q^ℓ) as follows:

$$\chi_w : x \mapsto \xi_p^{\text{tr}_{q^\ell/p}(wx)}, \qquad x \in \text{GF}(q^\ell), \tag{1.1}$$

where ξ_p is a primitive pth root of unity and $\text{tr}_{q^\ell/p}$ is the trace from GF(q^ℓ) to GF(p). It is easy to see that χ_w, $w \in \text{GF}(q^\ell)$, are all the characters of the additive group of GF(q^ℓ). These will be called additive characters of GF(q^ℓ).

0195–6698/00/080981 + 08 $35.00/0

For any nontrivial additive character χ_w of $\mathrm{GF}(q^\ell)$, we have

$$\begin{aligned}\chi_w(\Omega) &= (q-1)|w^\perp \cap \{y_1, y_2, \ldots, y_n\}| + (-1)(n - |w^\perp \cap \{y_1, y_2, \ldots, y_n\}|) \\ &= q|w^\perp \cap \{y_1, y_2, \ldots, y_n\}| - n, \end{aligned} \tag{1.2}$$

where $w^\perp = \{\langle y\rangle | y \in \mathrm{GF}(q^\ell), \mathrm{tr}_{q^\ell/q}(yw) = 0\}$, and $\mathrm{tr}_{q^\ell/q}$ is the trace from $\mathrm{GF}(q^\ell)$ to $\mathrm{GF}(q)$. We note that in the above calculation we have made use of the transitivity of trace. From (1.2) and Lemma 1.1, we have the following lemma.

LEMMA 1.2. *Let $\mathcal{O}$ and Ω be defined as above. Then $\mathcal{O}$ is a projective (n, ℓ, h_1, h_2) set in $PG(\ell-1, q)$ if and only if $\chi_w(\Omega) = qh_1 - n$ or $qh_2 - n$, for every nontrivial additive character χ_w, $w \in \mathrm{GF}(q^\ell)$. In other words, $\mathcal{O}$ is a projective (n, ℓ, h_1, h_2) set in $PG(\ell-1, q)$ if and only if Ω is a $(q^\ell, (q-1)n, \lambda, \mu)$ partial difference set in the elementary abelian group $(\mathrm{GF}(q^\ell), +)$, where $\lambda = (q-1)n + (qh_1 - n)(qh_2 - n) + q(h_1 + h_2) - 2n$, and $\mu = (q-1)n + (qh_1 - n)(qh_2 - n)$.*

An (m, r)-*arc* in $PG(2, q)$ is a set of m points, no $r+1$ of which are collinear. Let $\mathcal{K}$ be an (m, r)-arc in $PG(2, q)$, and let x be a point in A. Then each of the $(q+1)$ lines through x contains at most $r-1$ points of $\mathcal{K}$. Therefore

$$m \le 1 + (q+1)(r-1).$$

An (m, r)-arc is called *maximal* if $m = 1 + (q+1)(r-1)$. Any line of $PG(2, q)$ that contains a point of a maximal arc $\mathcal{K}$ evidently contains exactly r points of that arc; that is

$$|L \cap \mathcal{K}| = 0 \text{ or } r,$$

for any line L of $PG(2, q)$. Hence a maximal (m, r)-arc $\mathcal{K}$ in $PG(2, q)$ is a projective $(m, 3, 0, r)$ set in $PG(2, q)$.

For $q = 2^t$, Denniston [4] constructed maximal (m, r)-arcs in $PG(2, q)$ for every r, $r|q$, $r < q$ (see also [7, p. 304]). That is, he constructed projective $(1 + (q+1)(r-1), 3, 0, r)$ sets in $PG(2, q)$ for every $r = 2^s$, $1 \le s < t$. (We remark that for q odd, it was recently shown [1] that maximal arcs do not exist in $PG(2, q)$, when $r < q$.) In terms of partial difference sets (see Lemma 1.2), Denniston [4] constructed a $(2^{3t}, (2^{t+s} - 2^t + 2^s)(2^t - 1), 2^t - 2^s + (2^{t+s} - 2^t + 2^s)(2^s - 2), (2^{t+s} - 2^t + 2^s)(2^s - 1))$ partial difference set for every s, $1 \le s < t$, in the elementary abelian group $\mathbb{Z}_2^{3t}$. These parameters of partial difference sets will be called *Denniston parameters*.

As in the study of all other types of difference sets, one of the central problems in the study of partial difference sets is that for a given parameter set, which groups of the appropriate order contain a partial difference set with these parameters. In this paper, we investigate this problem for the Denniston parameters. We construct a family of $(2^{3t}, (2^{t+s} - 2^t + 2^s)(2^t - 1), 2^t - 2^s + (2^{t+s} - 2^t + 2^s)(2^s - 2), (2^{t+s} - 2^t + 2^s)(2^s - 1))$ partial difference sets in the group $\mathbb{Z}_4^t \times \mathbb{Z}_2^t$ when $s = t - 1$ and $s = 1$. One of the main ingredients of our construction is a class of Hadamard difference sets in the additive group of the Galois ring $GR(4, t)$. We remark that the idea of using ring structures to construct partial difference sets and other types of difference sets has been used successfully in recent years, see for example [2, 8–10, 14, 17].

2. GALOIS RING PRELIMINARIES

We need to recall the basics of Galois rings. Interested readers are referred to [12] for more details. We will only use Galois rings over $\mathbb{Z}_4$ in this paper. Let $\Phi_2(x) \in \mathrm{GF}(2)[x]$

be a primitive polynomial of degree t. Then there exists a unique polynomial $\Phi(x) \in \mathbb{Z}_4[x]$ of degree t such that $\Phi(x) \equiv \Phi_2(x) \pmod 2$, and $\Phi(x)$ divides $x^{2^t-1} - 1 \pmod 4$. Such a polynomial $\Phi(x)$ is called a *basic primitive* polynomial in $\mathbb{Z}_4[x]$. A *Galois ring over* $\mathbb{Z}_4$ *of degree* t, $t \geq 2$, denoted $GR(4, t)$, is the quotient ring $\mathbb{Z}_4[x]/\langle\Phi(x)\rangle$. We will use the shorthand $R = GR(4, t)$. If h is a root of $\Phi(x)$ in R, then $R = \mathbb{Z}_4[h]$ and the multiplicative order of h is $2^t - 1$.

The ring R is a finite local ring with unique maximal ideal $2R$, and $R/2R$ is isomorphic to the finite field GF(2^t). If we denote the natural epimorphism from R to GF(2^t) by π, then $g = \pi(h)$ is a primitive element of GF(2^t) $\cong R/2R$.

The set $\mathcal{T} = \{0, 1, h, h^2, \ldots, h^{2^t-2}\}$ is a complete set of coset representatives of $2R$ in R. This set is usually called a *Teichmüller system* for R. An arbitrary element α of R has a unique 2-adic representation

$$\alpha = \alpha_0 + 2\alpha_1,$$

where $\alpha_0, \alpha_1 \in \mathcal{T}$. The units in R have the form $h^i(1 + 2\xi)$, $0 \leq i \leq 2^t - 2$, $\xi \in \mathcal{T}$. We also note that, considered as vector spaces over GF(2), the maximal ideal $2R = \{0, 2, 2h, \ldots, 2h^{2^t-2}\}$ and GF(2^t) are isomorphic. An explicit isomorphism is given by $\phi : 2R \to$ GF(2^t), where $\phi(2h^i) = g^i$, $i = 0, 1, \ldots, 2^t - 2$, and $\phi(0) = 0$.

We will use tr : GF(2^t) $\to$ GF(2) to denote the usual trace map, and define $H_0 = \{x \in$ GF(2^t) | tr(x) $= 0\}$. A classical result of Singer [15] states that the hyperplanes of GF(2^t) are

$$H_0, H_1 = gH_0, \ldots, H_{2^t-2} = g^{2^t-2}H_0.$$

Therefore, all $(t - 1)$-dimensional GF(2)-subspaces of $2R$ are

$$K_0 = \phi^{-1}(H_0), K_1 = \phi^{-1}(H_1), \ldots, K_{2^t-2} = \phi^{-1}(H_{2^t-2}).$$

More explicitly, $K_0 = \{x \in 2R \mid \mathrm{tr}(\phi(x)) = 0\}$ and $K_j = h^j K_0$, $j = 1, 2, \ldots, 2^t - 2$.

The *Frobenius map* f from R to itself is the ring automorphism $f : \alpha_0 + 2\alpha_1 \mapsto \alpha_0^2 + 2\alpha_1^2$. This map is used to define the *trace* Tr from R to $\mathbb{Z}_4$, namely, $\mathrm{Tr}(\alpha) = \alpha + \alpha^f + \cdots + \alpha^{f^{t-1}}$, for $\alpha \in R$. The trace of a Galois ring can be used to define all of the additive characters of the ring, as demonstrated in the following well-known lemma.

LEMMA 2.1. *For $\beta \in R$, the function χ_β with $\chi_\beta(x) = \sqrt{-1}^{\mathrm{Tr}(\beta x)}$ for all $x \in R$ is an additive character of R, and every additive character of R is obtained in this way.*

For convenience of the reader, we include a proof here.

PROOF. First of all, it is clear that χ_β is an additive character of R since the trace map Tr is additive. Noting that Tr is not identically zero on R, we see that χ_1 is a nontrivial character. Therefore, if $\beta, \gamma \in R$ with $\beta \neq \gamma$, then

$$\frac{\chi_\beta(z)}{\chi_\gamma(z)} = \chi_1((\beta - \gamma)z) \neq 1,$$

for suitable $z \in R$, and so χ_β and χ_γ are distinct characters. So if β runs through R, we get 4^t distinct additive characters χ_β. On the other hand, R has exactly 4^t additive characters. Hence the list of additive characters of R is already complete. □

We note that in the above lemma if $\beta \in 2R\backslash\{0\}$, then χ_β is a character of order 2 and χ_β is principal on $2R$, and if $\beta \in R\backslash 2R$, then χ_β is a character of order 4 and χ_β is nonprincipal on $2R$. In the latter case, we write $\beta = (1 + 2\xi)h^i$ for $\xi \in \mathcal{T}$. We note that $\chi_\beta = \chi_{(1+2\xi)h^i}$

is principal on K_{-i}, where the subindex $-i$ should be viewed modulo 2^t-1, and $\chi_{(1+2\xi)h^i}$ is nonprincipal on all other K_j, $j \not\equiv -i \pmod{2^t-1}$.

We will need the following lemma which gives the 2-adic representation for the sum of two elements in the Teichmüller set $\mathcal{T}$ of R.

LEMMA 2.2. *Let $h^i, h^j \in \mathcal{T}$, $0 \le i, j \le 2^t-2$. The 2-adic representation of h^i+h^j is*

$$h^i + h^j = (h^i + h^j + 2\sqrt{h^{i+j}}) + 2\sqrt{h^{i+j}},$$

where $(h^i + h^j + 2\sqrt{h^{i+j}}) \in \mathcal{T}$ and $\sqrt{h^{i+j}} \in \mathcal{T}$.

PROOF. If we write $h^i + h^j = \alpha + 2\beta$ for $\alpha, \beta \in \mathcal{T}$, then

$$\alpha = \alpha^{2^t} = (\alpha+2\beta)^{2^t} = (h^i+h^j)^{2^t} = h^i + 2(h^i h^j)^{2^{t-1}} + h^j.$$

The last equality is true because all other terms in the binomial expansion of $(h^i+h^j)^{2^t}$ are 0 modulo 4 for $t \ge 2$. This implies the result. □

The final background we need for our construction is a 2-adic expansion of the trace $\mathrm{Tr}(ax)$. Let $a = 1+2\xi$, $\xi \in \mathcal{T}$, and $x \in \mathcal{T}$. Following the paper by Hammons *et al.* [6], we write the element $\mathrm{Tr}(ax)$ 2-adically,

$$\mathrm{Tr}(ax) = b_x + 2c_x,$$

where $b_x, c_x \in \{0,1\}$ are given as follows:

$$\begin{aligned} b_x &= \mathrm{tr}(\pi(x)), \\ c_x &= \sum_{0 \le i < j \le t-1} (\pi(x))^{2^i+2^j} + \mathrm{tr}(\pi(\xi x)), \end{aligned}$$

where π is the natural epimorphism from R to $R/2R$. (Strictly speaking, b_x, c_x are not in the field GF(2), they are in the subset $\{0,1\}$ of $\mathbb{Z}_4$. Here we abused the notation by identifying $\{0,1\} \subset \mathbb{Z}_4$ with the field GF(2).) We warn the reader that the above formulas for b_x, c_x are valid only for $x \in \mathcal{T}$.

The following lemma is straightforward and its proof can be found in [17].

LEMMA 2.3. *Let $Q(y) = \sum_{0 \le i < j \le t-1} y^{2^i+2^j}$ be a polynomial over* GF(2^t). *Then $Q(y+y^2) = \mathrm{tr}(y+y^3)$, for every $y \in \mathrm{GF}(2^t)$.*

3. CONSTRUCTION OF PDSs

We begin this section with a construction of a collection of Hadamard difference sets in the additive group of $R = GR(4,t)$. A Hadamard difference set in an abelian 2-group is a partial difference set with $v = 4N^2$, $k = 2N^2 - N$ elements, and $\lambda = \mu = N^2 - N$. In our case, $N = 2^{t-1}$, and the group has order 2^{2t}. In [13] and [5], McFarland and Dillon construct Hadamard difference sets as a union of cosets of hyperplanes of an elementary abelian subgroup H of order 2^t, where the coset representatives for the hyperplanes are from distinct cosets of H in the group. From Section 2, we see that the Galois ring $R = GR(4,t)$ has an elementary abelian subgroup $2R$ of the correct size 2^t, and we identified the hyperplanes of the subgroup $2R$ as K_j, $j = 0, 1, \ldots, 2^t-2$. Thus, in order to construct explicitly some Hadamard difference sets in R for our later use, we only need to find appropriate coset representatives for the K_j's. We will maintain the same notation as in Section 2 throughout this section.

THEOREM 3.1. *Let $w \in R/2R$ with* $\mathrm{tr}(w) = 1$, *and let $a_{i,j}$ be any element of R such that $\pi(a_{i,j}) = g^i(1+w) + g^j w$, $0 \le i,\ j \le 2^t - 2$. The set $E_i = \cup_{j=0}^{2^t-2}(h^i + h^{2i-j} + 2a_{i,j} + K_j)$ is a Hadamard difference set in the additive group $(R,+)$ with $N = 2^{t-1}$ for each i, $0 \le i \le 2^t - 2$.*

PROOF. Suppose $(h^i + h^{2i-j} + 2a_{i,j})$ and $(h^i + h^{2i-j'} + 2a_{i,j'})$ are in the same coset of $2R$ in R for $j \not\equiv j' \pmod{2^t - 2}$. This implies that $h^{2i-j} - h^{2i-j'} \in 2R$. However, this is not possible for two distinct elements of the Teichmüller system. Thus, the two coset representatives are in distinct cosets of $2R$, and hence the set E_i is a Hadamard difference set by the construction of McFarland and Dillon [5, 13]. □

REMARK. Since $2(h^{i-j} + h^{2i-2j}) \in K_0$, it follows that $2(h^i + h^{2i-j} + 2a_{i,j}) \in K_j$ for every j, $1 \le j \le 2^t - 2$. Therefore each E_i in the above theorem is reversible, i.e., $-E_i = E_i$, for each i, $0 \le i \le 2^t - 2$. We also note that the conditions on w and $a_{i,j}$ do not play a role in the proof of this theorem, but they will be important in later computations.

We are now ready to define our PDS in $\mathbb{Z}_4^t \times \mathbb{Z}_2^t$. Consider the group $G = (R,+) \times (GF(2^t),+) \cong \mathbb{Z}_4^t \times \mathbb{Z}_2^t$. Define

$$D = \cup_{i=0}^{2^t-2}(E_i, g^i),$$

where $(E_i, g^i) = \{(x, g^i) | x \in E_i\}$.

THEOREM 3.2. *The set D defined above is a* $(2^{3t}, (2^{2t-1} - 2^{t-1})(2^t - 1), 2^{t-1} + (2^{2t-1} - 2^{t-1})(2^{t-1} - 2), (2^{2t-1} - 2^{t-1})(2^{t-1} - 1))$ *partial difference set in $G \cong \mathbb{Z}_4^t \times \mathbb{Z}_2^t$.*

PROOF. We need to verify that for every nonprincipal character χ of G, the character sum $\sum_{d \in D} \chi(d) := \chi(D)$ is equal to $-(2^t - 1)2^{t-1}$ or 2^{t-1} as specified by Lemma 1.1. Every character of G can be written as $\chi_\beta \otimes \psi$, where χ_β is an additive character of R and ψ an additive character of $\mathrm{GF}(2^t)$, and

$$\chi_\beta \otimes \psi(D) = \sum_{i=0}^{2^t-2} \chi_\beta(E_i)\psi(g^i),$$

where $\chi_\beta(E_i) = \sum_{x \in E_i} \chi_\beta(x)$.

We distinguish the following cases.

(1) *χ_β principal, ψ nonprincipal.* $\chi_\beta \otimes \psi(D) = \sum_{i=0}^{2^t-2} |E_i| \psi(g^i) = -(2^{2t-1} - 2^{t-1})$. (We use the fact that the sum of a nonprincipal character over the nonidentity elements of a group is -1 here and throughout this proof.)

(2) *χ_β nonprincipal, ψ principal.* $\chi_\beta \otimes \psi(D) = \sum_{i=0}^{2^t-2} \chi_\beta(E_i)$. We consider two subcases. $\beta \in 2R \setminus \{0\}$: Since χ_β is principal on $2R$, $\chi_\beta(E_i) = 2^{t-1} \sum_{j=0}^{2^t-2} \chi_\beta(h^i + h^{2i-j})$; also χ_β induces an additive character on $R/2R = GF(2^t)$, which will be denoted by χ. Noting that $\chi(g^i) = \chi_\beta(h^i)$, we have

$$\begin{aligned}\chi_\beta(E_i) &= 2^{t-1} \sum_{j=0}^{2^t-2} \chi(g^i + g^{2i-j}) \\ &= 2^{t-1} \sum_{j=0}^{2^t-2} \chi(g^i)\chi(g^{2i-j})\end{aligned}$$

$$= 2^{t-1}\chi(g^i)\sum_{j=0}^{2^t-2}\chi(g^{2i-j})$$
$$= -2^{t-1}\chi(g^i).$$

Summing over all i, we get

$$\chi_\beta \otimes \psi(D) = \sum_{i=0}^{2^t-2}(-2^{t-1}\chi(g^i)) = -2^{t-1}(-1) = 2^{t-1}.$$

$\beta \in R\backslash 2R$: Let $\beta = (1+2\xi)h^{-\ell}$ for some $\xi \in \mathcal{T}$. By remarks following Lemma 2.1, we know that $\chi_{(1+2\xi)h^{-\ell}}$ is principal on K_ℓ and nonprincipal on all other K_j, $j \neq \ell$. Therefore,

$$\chi_{(1+2\xi)h^{-\ell}}(E_i) = 2^{t-1}\chi_{(1+2\xi)h^{-\ell}}(h^i + h^{2i-\ell} + 2a_{i,\ell})$$
$$= 2^{t-1}\sqrt{-1}^{\mathrm{Tr}((1+2\xi)(h^{i-\ell}+h^{2(i-\ell)}))}(-1)^{\mathrm{tr}(g^{-\ell}\pi(a_{i,\ell}))}.$$

Applying Lemma 2.2 to $h^{i-\ell} + h^{2(i-\ell)}$, we get

$$\mathrm{Tr}((1+2\xi)(h^{i-\ell} + h^{2(i-\ell)})) = \mathrm{Tr}\big((1+2\xi)(h^{i-\ell} + h^{2(i-\ell)} + 2\sqrt{h^{3(i-\ell)}})\big)$$
$$+\mathrm{Tr}(2\sqrt{h^{3(i-\ell)}}),$$

where $h^{i-\ell} + h^{2(i-\ell)} + 2\sqrt{h^{3(i-\ell)}} \in \mathcal{T}$.
Combining the 2-adic expansion of the trace $\mathrm{Tr}((1+2\xi)x)$ in terms of b_x and c_x and Lemma 2.3, we get

$$\mathrm{Tr}\big((1+2\xi)(h^{i-\ell} + h^{2(i-\ell)} + 2\sqrt{h^{3(i-\ell)}})\big)$$
$$= \mathrm{tr}(g^{(i-j)} + g^{2(i-\ell)}) + 2(Q(g^{i-\ell} + g^{2(i-\ell)}) + \mathrm{tr}(\pi(\xi)(g^{i-\ell} + g^{2(i-\ell)})))$$
$$= 2\mathrm{tr}(g^{i-\ell} + g^{3(i-\ell)} + \pi(\xi)(g^{i-\ell} + g^{2(i-\ell)}))$$

Here we should think the value of the trace in the last equality above is in $\{0, 1\} \subset \mathbb{Z}_4$, see the remarks following the 2-adic expansion of $\mathrm{Tr}((1+2\xi)x)$ in Section 2.
Returning to our computation of $\chi_{(1+2\xi)h^{-\ell}}(E_i)$ and using our choice for $\pi(a_{i,\ell})$ from Theorem 3.1, we get

$$\chi_{(1+2\xi)h^{-\ell}}(E_i) = 2^{t-1}(-1)^{\mathrm{tr}(g^{i-\ell}+g^{3(i-\ell)})}(-1)^{\mathrm{tr}(\pi(\xi)(g^{i-\ell}+g^{2(i-\ell)}))}$$
$$\cdot (-1)^{\mathrm{tr}(\sqrt{g^{3(i-\ell)}})}(-1)^{\mathrm{tr}(g^{-\ell}(g^i(1+w)+g^\ell w))}$$
$$= 2^{t-1}(-1)^{\mathrm{tr}(g^{i-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)}))}(-1)^{\mathrm{tr}(w)}$$
$$= -2^{t-1}(-1)^{\mathrm{tr}(g^{i-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)}))}.$$

We observe that $w + \pi(\xi) + \sqrt{\pi(\xi)} \neq 0$ for any $\pi(\xi)$ because by our choice of w, $\mathrm{tr}(w) = 1$ (see Theorem 3.1). This implies that

$$\sum_{i=0}^{2^t-2}(-1)^{\mathrm{tr}(g^{i-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)}))} = -1,$$

which shows that $\chi_{(1+2\xi)h^{-\ell}} \otimes \psi(D) = \sum_{i=0}^{2^t-2}\chi_{(1+2\xi)h^{-\ell}}(E_i) = -2^{t-1}(-1) = 2^{t-1}$.

(3) χ_β *nonprincipal*, ψ *nonprincipal*. As in the previous case, we distinguish two subcases.

$\beta \in 2R\backslash\{0\}$: Since χ_β is principal on $2R$, it induces a nonprincipal character χ on $R/2R$. Following the pattern of the previous computations, we get

$$\begin{aligned}\chi_\beta \otimes \psi(D) &= \sum_{i=0}^{2^t-2} \chi_\beta(E_i)\psi(g^i) \\ &= \sum_{i=0}^{2^t-2} 2^{t-1} \sum_{j=0}^{2^t-2} \chi_\beta(h^i + h^{2i-j})\psi(g^i) \\ &= \sum_{i=0}^{2^t-2} 2^{t-1} \sum_{j=0}^{2^t-2} \chi(g^i + g^{2i-j})\psi(g^i) \\ &= \sum_{i=0}^{2^t-2} 2^{t-1}\chi(g^i)\psi(g^i) \sum_{j=0}^{2^t-2} \chi(g^{2i-j}).\end{aligned}$$

The inner sum of the last line has the value -1 because it is a sum of a nonprincipal character over all of the nonidentity elements of the group. Thus, the sum reduces to $\sum_{i=0}^{2^t-2} -2^{t-1}(\chi\psi)(g^i)$. If $\chi\psi$ is principal, this sum is $-2^{t-1}(2^t-1)$, and if $\chi\psi$ is nonprincipal, the sum is 2^{t-1}.

$\beta \in R\backslash 2R$: Take $\beta = (1+2\xi)h^{-\ell}$ as in the previous case, and let $\psi(x) = (-1)^{\mathrm{tr}(cx)}$ for some $c \in GF(2^t)$, $c \neq 0$. Using our work from above, we get

$$\begin{aligned}\chi_{(1+2\xi)h^{-\ell}} \otimes \psi(D) &= -2^{t-1} \sum_{i=0}^{2^t-2} (-1)^{\mathrm{tr}(g^{i-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)}))}(-1)^{\mathrm{tr}(cg^i)} \\ &= -2^{t-1} \sum_{i=0}^{2^t-2} (-1)^{\mathrm{tr}(g^i(c+g^{-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)})))}.\end{aligned}$$

If $c + g^{-\ell}(w+\pi(\xi)+\sqrt{\pi(\xi)}) = 0$, then $\chi_{(1+2\xi)h^{-\ell}} \otimes \psi(D) = -2^{t-1}(2^t-1)$, and if $c + g^{-J}(w+\pi(\xi)+\sqrt{\pi(\xi)}) \neq 0$, then $\chi_{(1+2\xi)h^{-\ell}} \otimes \psi(D) = 2^{t-1}$.

By Lemma 1.1, this proves that the set D is a PDS with the parameters listed in the statement of the Theorem. □

REMARKS. (1). We may consider the dual of the partial difference set D in Theorem 3.2 in the following sense. Let G^* be the character group of G, where G is the group in Theorem 3.2. It is well-known that $G^* \cong G$. So $G^* \cong \mathbb{Z}_4^t \times \mathbb{Z}_2^t$. Define $D^- = \{\chi \in G^* \mid \chi \neq \chi_0, \chi(D) = -2^{t-1}(2^t-1)\}$. Then by a well-known theorem of Delsarte [3], D^- is a $(2^{3t}, (2^{t+s} - 2^t + 2^s)(2^t-1), 2^t - 2^s + (2^{t+s} - 2^t + 2^s)(2^s-2), (2^{t+s} - 2^t + 2^s)(2^s-1))$ partial difference set in G^* with $s = 1$. We note that the parameters $(2^{3t}, (2^t+2)(2^t-1), 2^t-2, 2^t+2)$ are the parameters of the partial difference sets corresponding to hyperovals in $PG(2, 2^t)$.

(2). We remark that the partial difference set in Theorem 3.2 is in the group $\mathbb{Z}_4^t \times \mathbb{Z}_2^t$. In contrast, the partial difference sets constructed by Denniston [4] are in the group $\mathbb{Z}_2^{3t}$. The methods of these two constructions are quite different. So it is very likely that the resulting strong regular graphs are nonisomorphic.

ACKNOWLEDGEMENTS

The research of Jim Davis was supported by a grant from Hewlett-Packard. The research of Qing Xiang was supported in part by NSA grant MDA 904-99-1-0012, and a grant from University of Delaware Research Foundation.

REFERENCES

1. S. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997), 31–47.
2. Y. Q. Chen, D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings. II, *J. Comb. Theory Ser. A*, **76** (1996), 179–196.
3. P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep.*, Suppl. No. 10.
4. R. H. F. Denniston, Some maximal arcs in finite projective planes, *J. Comb. Theory*, **6** (1969), 317–319.
5. J. F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, *J. Comb. Theory A*, **40** (1985), 9–21.
6. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inf. Theory*, **40** (1994), 301–319.
7. J. W. P. Hirschfeld, *Projective Geometries Over Finite Fields*, 2nd edn, Clarendon Press, Oxford, 1998.
8. Hou Xiang-dong, q-ary bent functions constructed from chain rings, *Finite Fields Appl.*, **4** (1998), 55–61.
9. K. H. Leung and S. L. Ma, Constructions of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.*, **22** (1990), 533–539.
10. K. H. Leung and S. L. Ma, Partial difference sets with Paley parameters, *Bull. London Math. Soc.*, **27** (1995), 553–564.
11. S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.*, **4** (1994), 221–261.
12. B. R. McDonald, *Finite Rings with Identity*, Dekker, New York, 1974.
13. R. L. McFarland, A family of difference sets in non-cyclic groups, *J. Comb. Theory A*, **15** (1973), 1–10.
14. D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, special issue dedicated to Hanfried Lenz, *Des. Codes Cryptogr.*, **8** (1996), 215–227.
15. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Am. Math. Soc.*, **43** (1938), 377–385.
16. R. J. Turyn, Character sums and difference sets, *Pac. J. Math.*, **15** (1965), 319–346.
17. Q. Xiang and J. A. Davis, Constructions of low rank relative difference sets in 2-groups using Galois rings, *Finite Fields Appl.*, **6** (2000), 130–145.

Received 8 September 1999 and accepted in revised form 2 June 2000

JAMES A. DAVIS
Department of Mathematics and Computer Science,
University of Richmond,
Richmond, VA 23173,
U.S.A.
E-mail: jdavis@richmond.edu
AND

QING XIANG
Department of Mathematical Sciences,
University of Delaware,
Newark, DE 19716,
U.S.A.
E-mail: xiang@math.udel.edu